E-MAIL USE POLICIES
ANNOTATED BIBLIOGRAPHY

December 1997

TABLE OF CONTENTS

I. SAMPLE POLICIES

Arizona Attorney General's Office. *Interim Electronic Mail Policy* (January 17, 1997).

> This working policy determines the parameters for the proper use, preservation, disclosure, and disposition of electronic mail in the attorney general's office. This policy does not allow for personal use, but does include a definition of a formal communication within the electronic mail framework.

Arizona State University. *ASU Electronic Messaging Services Acceptable Use Policy*. (May 2, 1996). http://www.asu.edu/it/fyi/internet/policies/use.policy.html

> A good, brief policy that outlines the reasons e-mail is provided at ASU and lists the acceptable and unacceptable uses of the system.

Bozich, Nancy. *Appropriate Use of County E-Mail and Voice Messaging Systems* Maricopa County Information Technology Telecommunications Department. (September 11, 1996).

> This memo outlines the acceptable uses of the county e-mail system by employees including descriptions of what is and is not considered acceptable use.

Draft: Electronic Mail Policy. Minnesota Supreme Court (December 20, 1995).

> The purpose of this draft judicial branch policy is to "strongly encourage" use of e-mail as an effective and efficient business tool, within the framework of Minnesota's *Rules of Public Access to Records of the Judicial Branch*. The policy is simple and straightforward, stating that e-mail is to be used for business purposes of the judicial branch but recognizing that e-mail will occasionally be used for personal messages. Users must employ good judgment in type, tone and content of messages, in line with accepted

standards of business conversation, and messages must withstand public scrutiny Several inappropriate uses are specified, and the policy states that use is subject to all other judicial branch personnel rules. The policy reserves the right of authorized staff to access the contents of messages for business purposes, but prohibits access to messages (snooping) in the absence of a valid business purpose.

Draft E-Mail Policy. Judicial Branch of the State of New Mexico. (Approved June 26, 1997). http://www.fscll.org/Email.htm

New Mexico's policy covers such standard subjects as use, disclosure, privacy and retention of records. Use must conform to New Mexico's Ethical Guidelines for Judicial Employees and to the Standards for Computer Use in the Judiciary. While allowing personal use, the policy strongly stresses separation of personal and judicial e-mail. Personal e-mail should be kept in folders marked 'PERSONAL' and employees are encouraged to store all messages by subject. E-mail encryption is permitted, with the caveat that the receiver may choose not to treat it as private. Another interesting rule requires sending e-mail to multiple recipients only when necessary and to the smallest group possible.

Edwards, Margaret Hart. *E-Mail Policy - Landels, Ripley & Diamond*. Court TV Legal Help. http://www.courttv.com/legalhelp/business/forms/937.html

A sample e-mail policy designed to assist corporations in developing guidelines for employees use of the e-mail system.

Electronic Mail (E-Mail) Policy at SUNY Potsdam. State University of New York at Potsdam. (Last Modified August 29, 1996). http://www.potsdam.edu/isd/policies/Email-Policy.html

This short e-mail policy focuses on who may obtain an account and exceptions to the general rule of e-mail confidentiality. The policy also applies SUNY Potsdam's "Information Technology Acceptable Use Policy" to e-mail.

Florida Office of the General Counsel. "Department of State Electronic E-mail Opinion." *Department of State Memorandum*. (November 9, 1995). http://www.dos.state.fl.us/dlis/barm/email.htm

The Office of the General Counsel addresses such topics whether e-mail messages are public records in Florida, if so, are they subject to the State Department's existing retention requirements, and as public records should Florida's State Department develop new rules for the administration of e-mail system. Anyone interested in the legal issues raised by the use of e-mail should read this opinion.

Frank, Randy. *University of Michigan E-Mail Policy*. University Of Michigan (April 1994). http://www.umich.edu/~policies

This comprehensive e-mail policy of the University of Michigan discusses who is covered by the policy, how it will be interpreted, your rights as a user, and guidelines for system administrators.

Maricopa County (Arizona). *Electronic Mail Policy A1608*. (February, 1997).

> This policy governs the use of e-mail for all Maricopa County employees. It provides for limited personal use of e-mail, places electronic mail messages within the framework of the Public Records laws, and defines different types of e-mail communications. The policy also sets areas of responsibility for both employees and management to assure for the security and smooth operation of the electronic mail system. At the end is an employee agreement form.

Moen, Charles. "UTMB Electronic Mail (E-Mail), Policy 2.13.6." *UTMB Records Managment Handbook*. University of Texas Medical Branch at Galveston (Last updated March 22, 1996). http://www.utmb.edu/biocomm/rm_hb4.htm

> The short e-mail policy states e-mail's lack of confidentiality, that the system should only be used for official state business, and that state public record laws apply to electronic mail. Other handbook sections detail Texas' Open Records Act, the State of Texas Records management program, and record management standards and procedures.

Office of Information Services - Office of Telecommunications Management. *State Information Transport Network Acceptable Use Policy*. State of Delaware. http://otmde1.state.de.us/otm/sitnlaw.htm

> This clear and comprehensive policy discusses the reasons electronic resources are made available to employees, acceptable and unacceptable uses of the system, the code of ethics for using these resources, and the penalties for violating this policy.

Personal Computer and Electronic Communication Media Use and Privacy. Olympia, WA: Office of the Administrator for the Courts (August 11, 1995).

> The 1995 memorandum states the Washington Supreme Court policies governing use of personal computers, the Court's network, e-mail and voice mail. A version of the policies with explanatory annotations is included. The policy restricts use of computers and electronic communications media to "purposes related to the business of the judiciary;" restricts software and databases to those approved by the Court's automation committee, legally acquired, and evidenced by a valid license; and prohibits use for enumerated purposes. The policies also address use of passwords, possibility of unauthorized access, backup and storage of e-mail messages, and authority to access employees' stored messages.

Ridley, Clarence H. "Company Internet (and E-Mail) Usage Policy - Form 15-6," in *Computer Software Agreements: Forms and Commentary*, rev. ed. Boston: Warren Gorham & Lamont, 1993.

> This very comprehensive set of guidelines will help employers develop an Internet policy that will protect both the employer and the employee. The agreements give examples of fair use, services available on the Internet, security issues, and how to effectively support Internet access. The section regarding use is clear, effective, and can be adapted to fit almost any business structure.

The Rush-Presbyterian-St. Luke's Electronic Mail Policy. Rush-Presbyterian-St. Luke's Medical Center (Last modified October 17, 1996). http://www.rush.edu/Rumba/email.html

> The Medical Center's one page policy discusses security, misuse and privacy issues. However, the Center regards e-mail as a "personal medium" and will not regulate message content, or monitor unless absolutely necessary. The Center also warns against e-mail forgery, chain letters, and sending confidential information over the system.

State of Washington. *Information Technology Policy Manual.* (Updated September 1997). http://www.wa.gov/dis/OITO/it_manual/

> This manual contains policies approved by the Information Services Board covering information technology acquisition, planning, disaster recovery, and security. The manual includes Electronic Message Privacy Guidelines in Washington State Government (September 1991), which provides a sample agency policy designed to assist in the development of employee use policies. The sample policy makes several interesting points including: the notion that electronic message systems are not a secure form of communication and as such the governing agency will not guarantee data confidentiality or integrity. The policy also includes some basic definitions.

University of California Draft Email Policy: Cover Letter. University of California, (September 29, 1997). http://www.ucop.edu/ucophome/policies/email/

> This cover letter explains the reasons for and summarizes the new University of California e-mail policy. Further white papers on information technology are at http://www.ucop.edu/irc/wp/wp_Contents.html.

University of California Office of the President Electronic Mail Policy. University of California. (Reissued March 23, 1998). http://www.ucop.edu/ucophome/policies/email/email.html

> This revised policy updates the university policy of August 1996. The new policy specifically defines what conditions will trigger non-consensual access to e-mail, and provides an appendix of definitions. Also provided are a list of references including state and federal statutes and other guidelines for the University of California. One interesting feature is the clarification of when a user has 'possession' of an e-mail record.

Warshawsky, Gale. *LLNL Computer Use Policy and Security Rules*. Lawrence Livermore National Laboratory, 1993.

> This is a listing of general computer use policies and security rules that apply to all personnel using LLNL computers on networks. Reading this article will give anyone writing policies of this nature useful tips on what should and should not be included.

II. E-MAIL POLICY DRAFTING CONSIDERATIONS

Calbiocem Electronic Mail - Policy. http://www.kensho.com/pubs/email/calbiochem-email-Policy.html

> This marketing piece provides examples of topics that should be included in an e-mail or Internet policy, including proper use, user rights, and responsible usage. It also describes how an inadequate e-mail policy may create problems and lists other Internet sites that could be of use to those drafting policies.

Colorado S.B. 96-212. Public records - open meetings - use of electronic mail - privacy interests - retention of records - requests for public access.

> This bill concerning access to governmental use of e-mail and state open meeting laws was passed and signed by the governor June 1, 1996. This new law amends several existing Colorado statutes regarding open meetings to reflect the advent of this new technology. Issues addressed include the use of e-mail by the members of the general assembly, elected officials, and state employees, the legality of disclosing e-mailed information, and whether messages need to be archived. A summary of S.B. 96-212 is available at the Colorado Legislative Assembly's 1996 Bills Digest: http://www.state.co.us/gov_dir/leg_dir/diggs.html.

Computer Professionals for Social Responsibility. *A Sample E-mail and Voice-mail Policy (with CPSR's Suggestions for Improvement).* CPSR Portland Chapter. (Last updated: August 27, 1997). http://www.cpsr.org/dox/program/emailpolicy.html

> CPSR sets out an Oregon computer company's policy and then critiques it. Among other suggestions, CPSR recommends that companies clearly state the level of e-mail monitoring, and discuss e-mail policies in terms of employee rights and values. CPSR also includes a labor union's comments on the policy, and a reminder that e-mail messages are organizational records.

Computer Security Institute. *CSI Manager's Guide to E-Mail Security* (1994).

> The guide describes how to provide employees with the benefits of e-mail without exposing the organization and its information to the many risks e-mail brings. It lists specific e-mail hazards, use of e-mail as evidence, legal implications of e-mail use, and how to protect your system and employees from illegal or unauthorized uses. An order form for this document can be found at: http://www.gocsi.com/m_form.htm

Florida Rules of Judicial Administration, Rule 2.051. Public Access to Judicial Records. http://www.gate.net/~wyman/flo/fla.r.jud.admin.html#2.051

> Rule 2.051 defines judicial records as including any "material created by any entity within the judicial branch, regardless of physical form, characteristics, or means of transmission, that are made or received...in connection with the transaction of official business by any court or court agency." The rule sets out exemptions, and a review

process for denial of access requests. An extensive commentary discusses the use of electronic mail within the judicial branch, as a "judicial record" under the rule, concluding that while, with some exceptions, electronic mail (as well as use of online legal research services such as Westlaw) within a court's jurisdiction would be exempted, some electronic mail, particularly that between a court and persons outside the court's jurisdiction, would be non-exempt, and each court should establish the means to make a record of non-exempt electronic mail. The commentary also recommends that courts publish an electronic mail address for public access, with individual mail addresses remaining exempt from disclosure. The URL provided here is to an unofficial version of the Florida Rules "provided for informational purposes only" by Florida Law Online.

Guttman, Barbara, and Robert Bagwill. *NIST Special Publication 800-XX Internet Security Policy: A Technical Guide.* National Institute of Standards and Technology. (July 21, 1997). http://csrc.nist.gov/isptg/html/

NIST has developed the complete guide for creating a secure Internet policy. Section 8 discusses the technical aspects of e-mail as well as detailing e-mail safeguards and protections. Further sections cover archiving requirements for federal agencies and companies. Section 8.8 also provides a sample e-mail policy that would thoroughly address security concerns. An appendix at the end lists other resources for Internet security.

Hillis, Bradley J. "Approaches to Internet Access: A Primer for Managers of Courts and Law Firms." *ILP Newsletter* (January 20, 1997). http://www.collegehill.com:80/ilp-news/hillis.html

Hillis reviews the options available for allowing employee access to the Internet. A manager may provide access E-mail access only, Telnet (text -only, without e-mail) access, or complete access to the Internet. E-mail allows employees to send documents to one another, and requires little training, but leaves great amount of litter and lends itself to unproductive personal use. Telnet access permits the searching of some statutes and world wide card catalogs but not the full text of books or periodicals listed. Telnet also removes some of the security concerns associated with the world wide Web. Only open access to the Web allows full use of the electronic resources available. Security measures such as a firewall can provide full access without some of the risks, but do increase the cost of using the Internet. Hills concludes even limited access is better than none and provides a list of useful Telnet sites.

Leinfuss, Emily. "Policy Over Policing." 18 *Info World* 55 (August 19, 1996).

The fast pace of technological change makes it difficult for organizations to develop consistent e-mail and Internet use policies. This article provides examples of ways for companies to provide access to these services and still protect their rights and the rights of their employees.

National Archives and Record Administration. "Electronic Mail Systems; General Record Schedule 20; Disposition of Electronic Records; Final Rule and Notice." 60 *Federal Register* 44633 (August 28, 1995). http://www.access.gpo.gov/su_docs/aces/aces140.html

These are the proposed National Archives and Records Administration standards for the management of federal records created or received via electronic mail. These standards will affect all Federal agencies and amend 36 CFR Chapter XII. This document outlines the proposed standards, includes comments made by interested parties to the proposed rules and the responses made by NARA. The document also takes a good look at the problems associated with the retention and access to electronic records. Any agency facing these issues should consider some of the recommendations made by this agency.

Natoli, James G. *Governor's Task Force on Information Resources Management Technology Policy 96-14: New York State Use of Electronic Mail.* (June 11, 1996). http://www.irm.state.ny.us/policy/tp_9614.htm

The state policy defines e-mail, and then suggests guidelines for agencies to formulate individual agency policies. Each agency policy should include sections on proper use, agency control of e-mail, and which state and federal laws apply. The policy encourages agencies to contact the State Archives and Records Administration (SARA) for training and assistance. Agencies should also consult the state archives publication *Managing Records in E-Mail Systems* for further guidelines.

Power, Richard. "Security in the Digital Age." 15 *Digital Age* 20 (January 1996).

This article is an overview of security programs in the emerging corporate setting of increased internetworking and distributed systems. The author identifies three common shortcomings of security planning: failure to understand the scope of the risks and vulnerabilities, disproportionate concern about Internet security and firewalls, and over-reliance on technology for system security. To address these, he advocates preparation of strong, enforceable written policies for applications such as e-mail, attention to physical systems security, development and testing of emergency response plans, and attention to end users (increasing their awareness of and responsibility for security, and monitoring of workstation practices).

Report of the Ad Hoc Committee on the Appropriate Use of E-mail for the University of Texas at Austin. The University of Texas at Austin, April 1994. http://www.utexas.edu/policies/email

The report provides a general background to the Univerity's 1994 e-mail policy. Topics covered include a definition of the Internet, discussion of the policy, and survey responses from other universities.

Report of the Electronic Mail Task Force. Prepared for the Office of Management and Budget, Office of Information and Regulatory Affairs, April 1, 1994. http://snyside.sunnyside.com/cpsr/government_info/info_access/PROFS_CASE/E-Mail_Policy_in_Federal_Gover

The Federal Government developed this comprehensive report to aid agencies and departments in drafting e-mail policies. The report discusses the federal government goal of a "single, unified electronic postal system" that is both trustworthy and reliable. To that end, functional, management, and technical requirements are considered, as well as the legal and policy issues associated with e-mail use. The Task Force includes a separate section on when government agency monitoring would be appropriate. Other issues covered are privacy, Freedom of Information issues, security and permissible use.

Appendixes provide a copy of the E-Mail Task Force charter, a memorandum on solicitation for information, and an e-mail policy checklist.

United States Court of Appeals for the Third Circuit. Appendix 1. Internal Operating Procedures. Chapter 4. *Panel Conference Procedure.*

This chapter outlines the procedure for the use of e-mail by judges in a panel decision.

III. ISSUES

Allison, G. Burgess. "E-mail Security on the Internet." *Law Practice Management - Technology Update* (April 1996). http://www.abanet.org/lpm/magazine/tu963.html#tag0

Burgess discusses the issue of Internet security and the pros and cons of sending e-mails via the Net. The article also addresses the current fear of the Internet and the validity of this line of thought.

Baumhart, Julia Turner. "The Employer's Right to Read Employee E-Mail: Protecting Property or Personal Prying?" 8 *The Labor Lawyer* 849 (1982).

This article considers the extent to which the Electronic Communications Privacy Act of 1986, the federal wiretap law and privacy rights under state and constitutional law limit the employers' right to read e-mail. The article interprets the 1986 ECPA statute to allow the private employer limited rights of interception as part of normal business procedure when necessary to protect employers' property rights in the system or to provide e-mail service. The article also reviews issues of employee consent, the responsibilities of government employers, and the possible effects of existing tort and search and seizure cases on an e-mail situation. At the end, Baumhart suggests that employers limit monitoring to message status rather than content, state explicitly in the handbook employers' right to monitor e-mail, and warn employees that passwords and deletion do not safeguard employee messages from monitoring.

Beckman, David, and David Hirsch. "E-Mail Rules to Live By." 83 *ABA Journal* 78 (August 1997).

Two law firm partners list what they consider to be the six most important rules governing e-mail use in the law office. Among them, Beckman and Hirsch suggest keeping e-mail from home at home, keeping e-mail short and to one topic, and avoiding accidental duplication through copying to more than one list.

Behar, Richard. "Who's Reading Your E-Mail?" *Fortune* (February 3, 1997). http://pathfinder.com/@@NWN52AYAzpgloEfx/fortune/1997/970203/eml.html

Even the most sophisticated computer security systems are vulnerable to attacks by hackers. This article details the average hacker's background and methods together with the measures taken by companies to defeat them. The article also advises companies

thwart hackers by scrambling messages through encryption software and ensuring its employees choose hard to guess computer passwords.

Brandriss, Ira L. "Writing in Frost on a Window Pane: E-Mail and Chatting on Ram and Copyright Fixation." 43 *Journal of the Copyright Society of the U.S.A.* 237 (1996).

Brandriss provides a readable and intriguing discussion of the laws of copyright currently applied to e-mail and other electronic writings. The article focuses on analogies of the e-mail writing process, the original purposes of copyright, and how they affect the law on e-mail and Internet document reproduction today. After examining the legal definitions of 'writing' and 'fixation', Brandriss concludes that e-mail messages are not permanent enough to be copyrighted without changing the meaning of the copyright law. The "unauthorized on-line browsing", however, could be fixed enough to be copyright infringement. Brandriss suggests that, among other changes, the law be amended to distinguish between a writing fixed enough for editing and a writing fixed enough for copying.

Brown, Eryn. "The Myth of E-Mail Privacy." *Fortune* (February 3, 1997). http://pathfinder.com/@@NWN52AYAzpgloEfx/fortune/1997/970203/eml.html#privacy

This short feature details the tenacity of deleted e-mail and the ease with which an employer or co-worker can access private messages. Don't ever expect privacy sending messages by company e-mail.

Brown, Robin. "FOCUS: Businesses Can Avoid Lawsuits Through Wise E-Mail Policies." 18 *New Orleans CityBusiness* 21 (July 14-20, 1997).

Brown briefly reviews the problem of the e-mail joke and what employers are doing to prevent e-mail's misuse. The author also discusses the New Orleans' city government's attempts to create a unified e-mail policy.

Bryant, Mary L. "E-Mail: Come Out And Play." *Solo* (Fall 1996).

The author finds that e-mail, while clearly having its downside, has improved communication in the law office, from the ability of clients to "talk" about their questions and concerns (and the lawyer's ability to document questions and responses) to the speed and ease of querying and responding to colleagues.

Cameron, James. "Internet E-mail In Law Office." 50 *Washington State Bar News* 44 (March 1996).

The author catalogs some of the important benefits of Internet e-mail: cheaper cost than telephone, fax or courier; ability to transfer documents; forum for finding information, sharing ideas, and networking; improved client services; and marketing. He then briefly describes a few of the most commonly available e-mail packages, including Qualcomm's Eudora and Netscape's e-mail program.

Dichter, Mark S. and Michael S. Burkhart. *Electronic Internaction in the Workplace: Monitoring, Retrieving and Storing Employee Communications in the Internet Age.* Morgan, Lewis & Bockius LLP, 1996. http://www.mlb.com/speech1.htm

> This paper prepared for the American Employment Law Council's fourth annual conference addresses employee e-mail monitoring issues. The authors provide a basic summary of the Internet and e-mail use before discussing federal and state laws that apply to monitoring. Section III discusses employers' liability for employee use of e-mail in defamation and sexual harassment actions and includes some recent (1996) case law. Further sections cover the effects of e-mail on union activities and warn how e-mail can cause the unauthorized disclosure of confidential information. The use of e-mail as evidence in litigation is also discussed.

Dutcher, William. "You Can't Get There From Here." 13 *PC Week* N5 (April 29, 1996).

> The Internet can increase productivity, but employee abuse can waste even more time than computer games. Few access-control methods are foolproof, but most will work reasonably well in conjunction with Internet usage policies. Dutcher discusses methods of controlling usages and provides descriptions of tools available to assist employers.

Fiscus, Chris. "Council May Give Public Access to E-mail." *Arizona Republic* B1 (October 8, 1996).

> This article discusses the new plan developed by the Phoenix City Council to provide the public with access to e-mail records sent from on council member to another. This new policy is to help prevent the possibility of council members holding a meeting via e-mail messages without the public being aware of the conversations. There are new and important implications for the governments' use of e-mail as a form of communications and the outcome of this proposal should be noted.

Frenkel, Ephraim. "Electronic Mail: High-Tech Communication, Unified Messaging Is The New Wave." 215 *New York Law Journal* S2 (February 26, 1996).

> This article presents readers with a very basic guide to e-mail. Frenkel aims this work at those readers who have little or no understanding of what e-mail is or how it works. The basic technology is explained and the benefits and problems of using this form of communication are discussed. Frenkel ends by providing readers with a basic users guide to e-mail which explains how to compose a message and gives a glossary containing some of the more standard abbreviations. A good article for anyone who is not currently e-mail literate.

Glassberg, Bonnie C., William J. Kettinger and John E. Logan. *A Conceptual Model of the Effect of Privacy, Ethical and Policy Concerns on Electronic Mail Usage* (Last Modified: September 24, 1997). http://hsb.baylor.edu/ramsower/acis/papers/glassb2.htm

> This paper takes a sociological approach to consider how employee and management attitudes will affect e-mail usage. The authors provide a model based on privacy and ethical concerns to predict the ideal policy. Among other predictions, they conclude that usage will increase when the e-mail policy matches the person's vision of the ideal e-mail policy.

Greenberg, Thomas R. "E-Mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute." 44 *American University Law Review* 219 (1994).

> Greenberg surveys the antecedents of the 1986 Electronic Communications Privacy Act of 1986, then analyses the elements of the statute. He considers cases on interception, voice mail cases, and the "ordinary course of business" exception. He also examines what would make employers liable under the ECPA.

Hammitt, Harry. "Coping with E-Mail Records." *Government Technology Magazine* (August, 1996). http://www.govtech.net:80/1996/gt/aug/aug1996-access/aug1996-access.htm

> Hammit's useful article covers e-mail issues important to government agencies and businesses. Hammit discusses such topics as whether to make paper copies, how long to store the electronic version, and whether a printed version is the same as the electronic version. The legal issues surrounding the use of e-mail are just emerging and this article provides insights into some of these new problems.

Hash, Paul E., and Christina M. Ibrahim. "E-Mail, Electronic Monitoring, and Employee Privacy." 37 *South Texas Law Review* 893 (1996).

> This article discusses the issues created by employee e-mail monitoring. Employers want to ensure productivity, but employees fear abuse of the privilege. Hash and Ibrahim survey the Electronic Communication's Privacy Act of 1986 (ECPA) and other laws protecting employee rights and conclude that current legislation favors employers' right to monitor over employee privacy rights. They suggest employers can further protect themselves from liability by placing the e-mail policy in the company handbook, and informing employees that e-mail and other electronic communications are strictly for business use, non-work related use is at their own risk, and that by using company equipment employees consent to monitoring.

Kadaba, Lini S. "Buried in E-Mail: Businesses Learn Timesaving Technology can Waste Time When Unimportant Messages Pile Up." *Knight-Ridder Newspapers* (September 18, 1996).

> This article discusses the problems inherent with the use of e-mail by employees in both professional and personal situations. Kadaba describes how system can become overloaded by improper use and outlines ways companies can deal with the situation.

Lange, Larry. "Is Big Brother Stalking the Net?" 906 *Electronic Engineering Times* 1 (June 17, 1996).

> Efforts to regulate the Internet are raising concerns that users' "cyber-rights" will be violated, and Internet users will suffer from censorship and lack of privacy. Lange describes the steps the Federal Government is taking to prevent illegal activities from occurring on the Internet.

Lee, Laurie Thomas. "Watch Your E-Mail! Employee E-Mail Monitoring and Privacy Law in the Age of the 'Electronic Sweatshop'". 28 *John Marshall Law Review* 139 (1994).

> Lee reviews the prevalence of e-mail in the work world, then considers the state and federal statutes which govern employee e-mail privacy rights. Lee argues that current legislation offers little protection to employees due to the law's ambiguities and permitted exceptions. The author next applies the existing common law on privacy to employee e-mail monitoring and then discusses proposed legislative solutions that would favor employees over employers. The article also lists state constitutions granting a privacy right, and state codes that have adopted wiretapping statutes' major exceptions.

Leibowitz, Wendy R. "Communication in the E-Mail Era: Deciphering the Risks and Fears." *National Law Journal* B9 (August 4, 1997).

> Leibowitz considers how the attorney-client privilege applies to e-mail messages. She concludes that e-mail is just as secure as the telephone or fax, though subject to the same risks of misdelivery and theft. The small amount of case law discussing the Internet suggests that courts will develop new principles for Internet use, rather than treat it as a variation of older forms of communication.

Leibowitz, Wendy R. "'Can We Talk?' E-Mail Is Ethics Maze." *National Law Journal* A1 (August 18, 1997).

> This article takes a closer look at attorneys' concerns that communicating with clients via e-mail could accidentally waive the attorney-client privilege. The article discusses ethics rulings issued by different states on the subject and the need for e-mail message encryption to protect privacy.

Leinfuss, Emily. "Policy Over Policing." 18 *InfoWorld* 55 (August 19, 1996).

> Leinfuss discusses corporate e-mail and Internet policy development. Technological change makes it difficult to develop consistent e-mail and Internet use policies. Primary areas of concern are privacy and security. The author states organizations have a legal right to access employee e-mail, but employees still need a guarantee of some level of privacy. Companies also have a legal responsibility to post policies and to provide written documentation for e-mail use. The author recommends the Electronic Messaging Association's white paper on developing an e-mail policy, and Baseline Software's *Information Security Policies Made Easy* which provides more than 700 policies and policy templates, and suggests Information Services managers join in developing privacy and security policies, develop retention policies that are amenable to IS and to the company, and create audit procedures.

Maurer, Betsy K. *Electronic Communication: Appropriate Use, Privacy and Surveillance.* Williams, Kastner & Gibbs LLP, 1996. http://www.wkg.com/resources/labor_employment/email.htm

> Maurer suggests ways that employers can protect themselves from liability while still allowing employees access to e-mail, voice mail, and the Internet. The author

summarizes employee monitoring issues and provides practical tips on drafting and enforcing an e-mail policy.

Miller, Brian. "Should Agencies Archive E-Mail?" *Government Technology Magazine* (February, 1995). http://www.govtech.net:80/1995/gt/feb/e-mail.htm

Miller discusses the new laws being developed at both the state and federal level regarding the use of e-mail by government employees. The article includes specific examples such as the development of the Florida Sunshine laws as well as case law on the subject.

Pollock, Bruce G. "Computing For The Small Law Office - Free E-Mail." 45 *Rhode Island Bar Journal* 23 (October 1996).

A very short article on the definition of e-mail that describes how e-mail can be beneficial to firms, and how to go about getting free e-mail service. Pollock outlines the basic computer resources needed to access the Internet and the free e-mail services and then goes on to inform readers how to go about obtaining this free service.

Rogers, Joan C. "Malpractice Concerns Cloud E-Mail, On-Line Advice." *ABA/BNA Lawyers' Manual on Professional Conduct* (March 6, 1996).

Rogers provides readers with an in-depth analysis on the problems associated with the use of e-mail by attorneys and outlines some of the ethical rules and considerations that need to be taken into account by any attorney who is planning on using this form of communication. Issues such as attorney-client privilege, encryption, confidentiality, and conferences are discussed and some suggestions on how to handle these issues are presented. This is a very thorough analysis of a complex problem and would be of use to any attorney who uses technology to communicate.

Ross, Susan B. "How Attorneys Are Changing the Way They Communicate." 1 *Internet Legal Practice Newsletter* (July 19, 1996). http://www.collegehill.com:80/ilp-news/ross-email.html

Ross provides readers with a look at how attorneys across the country are using e-mail to help develop and expand their services. In addition she shows how e-mail can be used to make the daily work flow more effective and efficient. The article does address some of the problems associated with the use of e-mail and provides some suggestions on how to solve these issues. An interesting look at how e-mail can be used effectively by attorneys.

Shear, Kenneth R. "Connecting to Damages." *Intellectual Property* (Winter 1996). http://www.ipmag.com/shear.html

This article deals with the legal framework surrounding e-mail use by corporations and organizations and the implications in the areas of personal privacy, libel, copyright and other wrongful acts. This is a new area within the legal area and this article spells out some of the key decisions regarding these topics.

Shear, Kenneth R. "What You Don't Know Can Hurt You." 43 *Louisiana Bar Journal* 464 (February 1996).

> Shear considers how the Electronic Communications Privacy Act (ECPA) of 1986 could prevent companies from monitoring employees' e-mail communications. He compares the violation of privacy case *Deal v. Spears* (which dealt with unlawful recording of telephone calls) to an e-mail monitoring situation and suggests possible damages.

Shein, Esther. "Big Brother?" 13 *PC Week* 43 (July 29, 1996).

> Many companies use monitoring tools to note or even restrict unproductive use of the Internet. However this raises concerns over users' lack of privacy, especially when a company does not have an official Internet use policy.

Singletary, Michelle. "E-Mail Punchlines Carry a Price." *Washington Post* A01 (March 18, 1997)

> This article discusses the dangers of treating employee E-Mail as casual conversation. The article describes how company employees often send racially or sexually biased jokes over the Internet, not realizing that such messages can be monitored by their employers or retrieved from backup systems after deletion. E-mail messages are also being increasingly used as evidence in discrimination and sexual harassment lawsuits. The article notes that legal experts have warned companies to develop a written e-mail usage policy and to prohibit offensive language and jokes in e-mail communications. Training should also be provided on how to use the system.

Smith, Arthur L. *E-Mail And The Attorney-Client Privilege*. Law Practice Management Committee of the Bar Association of Metropolitan St. Louis Web Page, 1995. http://bamsl.org/lpm/email.htm

> Smith provides readers with an overview of some of the problems associated with the use of e-mail by attorneys and presents some basic suggestions on how to avoid the problems. The article also outlines some to the basic legal tenets that must be considered before using these systems. A basic, but useful overview on the use of e-mail in the legal profession.

Stipe, Suzanne. 'Establish E-Mail Policy to Avoid Legal Pitfalls." 97 *Best's Review* 92 (July 1996).

> This short article discusses the need for a company e-mail policy. The article finishes with a series of guidelines for acceptable use. According to Stipe's sources, e-mail guidelines should include data security procedures and "virus awareness" as well as general rules on access and use and rules for communications outside the company network.

Thompson, Amy, and Sherry Harowitz. "Taking a Reading on E-Mail Policy." 40 *Security Management* 55 (November 1996).

> Thompson and Harowitz discuss the results of a Security Management survey on e-mail. In 1996, less than half of the company's responding had an e-mail policy in place. The authors polled all companies on e-mail policy elements, usage restrictions, archiving

requirements, and other aspects of e-mail use. They consider the survey results and then the policies of specific companies.

Trickey, Fred. "E-Mail Policy By the Letter." 40 *Security Management* 69 (April 1996).

Columbia University's Information Services security officer Trickey sets out the components of a secure company e-mail policy. Among other recommendations Trickey suggests obtaining the legal department's approval of the policy, clearly stating usage restrictions, and explaining the company's position on monitoring.

Van Doren, Jeffrey. "If You Monitor Company E-Mail, Have a Policy in Place." 15 *Pittsburgh Business Times* 14 (October 2, 1995).

This 1995 article briefly discusses some of the general dangers of monitoring employees' e-mail without a policy and then suggests ways to create and enforce a company policy.

White, Jarrod J. "E-Mail@Work.com: Employer Monitoring of Employee E-Mail." 48 *Alabama Law Review* 1079 (1997).

White provides another in-depth discussion of the current law on e-mail monitoring. The author surveys the relevant federal and state legislation from an employer's viewpoint, and then considers the possible liability from an employee common law privacy claim. White also reviews the former 1993 Privacy for Consumers and Workers Act that failed to pass in the Senate. At the end, White recommends employee involvement in the drafting of company e-mail policies, adequate publication of the policy, and employer restraint in exercising e-mail monitoring privileges.

IV. ADDITIONAL RESOURCES

E-Mail Guideline Development Task Force Research Library. Association of Records Managers International Standard Advisory and Development Committee (SAD). (No date given). http://www.orst.edu/Dept/archives/misc/wvbiblio1.html

ARMA discusses its goal of creating an industry-wide e-mail guideline and provides links to fourteen e-mail articles and reports as well as a series of other websites with e-mail documents. The collection is especially strong on materials from British Columbia.

Municipal Research and Services Center of Washington Library. *Internet Usage and E-Mail Policies.* Washington Library. (May 1997). http://www.mrsc.org/library/compil/cpemail.htm

The Washington Library compiled this collection of government agency e-mail policies and supplementary articles. Policies focus mainly on municipal and state agencies in Washington and the western states, with supplementary articles from administrative orders and newsletters.

Noonan, Dana. "Cybermail Nightmares and Daydreams." *The Piper Letter* (June 17, 1996). http://www.piperinfo.com/pl02/knot.html

> This special report of the Piper Letter describes basic problems associated with e-mail and suggests some electronic readings and websites that deal with the legal, organizational and security is sues.

Veeder, Stacy B. *Untitled Bibliography.* (Compiled December 1991). http://www.eff.org/pub/Privacy/Email_GII_NII/email_privacy.biblio

> Veeder has compiled an extensive e-mail bibliograpy for articles published from 1986 to 1991. Citations deal with employee and legal issues reported in newspapers and computer magazines. The bibliography is included in the Electronic Frontier Foundation's EFF "Privacy - Email/Network/NII/GII" Archive.
